

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

In the Matter of the Search of:

**Information, including the content of communications,
associated with the Instagram usernames listed
in Attachment A and collectively referred to as
SUBJECT ACCOUNTS, that are stored at the
premises Controlled by Meta Platforms, Inc.**

)
)
)
)
)
)
)

Case No: 2:24-mj-329

Magistrate Judge: Deavers

UNDER SEAL

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Matthew W. Guinn, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

EDUCATION TRAINING AND EXPERIENCE

1. I am a SA with the FBI and have been since April 2012. I am currently assigned to the Child Exploitation and Human Trafficking Task Force Crimes Against Children Squad, Cincinnati Division, Columbus Resident Agency. I am primarily responsible for investigating internet crimes against children, including child pornography offenses and the online exploitation of children.
2. During my career as a SA, I have participated in various investigations involving computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, digital media, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses involving children. As part of my duties as a SA, I investigate criminal violations relating to child exploitation and child pornography, including the online enticement of minors and the illegal production, distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422.
3. As a SA with the FBI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

PURPOSE OF THE AFFIDAVIT

4. I make this affidavit in support of an application for a search warrant for information associated with the following Instagram usernames and ID's:

- i. raven_cowther09 (Target: 6616303182)
- ii. ca_ssie800 (Target 59851155659)

(collectively the **SUBJECT ACCOUNTS**) that is stored at premises owned, maintained, controlled, or operated by Instagram, LLC, ("Instagram") a social-networking company owned by Facebook, Inc. and headquartered in San Francisco, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Instagram, LLC via Facebook, Inc. to disclose to the government records and other information in its possession, including the contents of communications, pertaining to the subscriber or customer associated with the **SUBJECT ACCOUNTS**.

5. The **SUBJECT ACCOUNTS** to be searched is more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, 2252A – the sexual exploitation of a minor, possession of child pornography, as well as 18 USC § 875(d) – extortion via interstate communications. I am requesting authority to search the **SUBJECT ACCOUNTS**, wherein the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.
6. The facts set forth below are based upon my knowledge, experience, observations, and investigation, as well as the knowledge, experience, investigative reports, and information provided to me by other law enforcement agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every known fact to me relating to the investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, 2252A – the production, distribution, transmission, receipt, and/or possession of child pornography and the coercion and enticement of a minor, as well as 18 USC §875(d) –

extortion via interstate communications extortion via interstate communications are presently located in the **SUBJECT ACCOUNTS**. I have not omitted any facts that would negate probable cause.

APPLICABLE STATUTES AND DEFINITIONS

7. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.
8. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.
9. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of

interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

10. Title 18, United States Code, Section 875, makes it a federal crime for any person to, with the intent to extort from another person, firm, association, or corporation, any money or thing of value, to transmit in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee of another.
11. As it is used in 18 U.S.C. § 2252A(a)(2), the term “child pornography”¹ is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
12. As it is used in 18 U.S.C. §§ 2251 and 2252, the term “sexually explicit conduct” is defined pursuant to Title 18, United States Code, Section 2256(2)(A) as “actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person.”
13. The term “sexually explicit conduct” has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), “sexually explicit conduct” also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or

¹ The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B hereto, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. §§ 2251 and 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

lascivious simulated (i) bestiality, (ii) masturbation, or (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

14. The term “minor”, as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as “any person under the age of eighteen years.”
15. The term “graphic,” as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean “that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.
16. The term “visual depiction,” as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.”
17. The term “computer”² is defined in Title 18 U.S.C. § 1030(e)(1) and 2256(6) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
18. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
19. “Cellular telephone” or “cell phone” means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless

telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.

20. “Internet Service Providers” (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
21. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

BACKGROUND INFORMATION REGARDING SOCIAL MEDIA AND INSTAGRAM

22. From my review of publicly available information provided by Instagram about its service, including Instagram’s “Privacy Policy,” I am aware of the following about Instagram and about the information collected and retained by Instagram.
23. Instagram owns and operates a free-access social-networking website of the same name that can be accessed at <http://www.instagram.com>. Instagram allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and other information. Users can access Instagram through the Instagram website or by using a special electronic application (“app”) created by the company that allows users to access the service through a mobile device.
24. Instagram permits users to post photos to their profiles on Instagram and otherwise share photos with others on Instagram, as well as certain other social-media services, including

Flickr, Facebook, and Twitter. When posting or sharing a photo on Instagram, a user can add to the photo: a caption; various “tags” that can be used to search for the photo (e.g., a user made add the tag #vw so that people interested in Volkswagen vehicles can search for and find the photo); location information; and other information. A user can also apply a variety of “filters” or other visual effects that modify the look of the posted photos. In addition, Instagram allows users to make comments on posted photos, including photos that the user posts or photos posted by other users of Instagram. Users can also “like” photos.

25. Upon creating an Instagram account, an Instagram user must create a unique Instagram username and an account password. This information is collected and maintained by Instagram.
26. Instagram asks users to provide basic identity and contact information upon registration and also allows users to provide additional identity information for their user profile. This information may include the user’s full name, e-mail addresses, and phone numbers, as well as potentially other personal information provided directly by the user to Instagram. Once an account is created, users may also adjust various privacy and account settings for the account on Instagram. Instagram collects and maintains this information.
27. Instagram allows users to have “friends,” which are other individuals with whom the user can share information without making the information public. Friends on Instagram may come from either contact lists maintained by the user, other third-party social media websites and information, or searches conducted by the user on Instagram profiles. Instagram collects and maintains this information.
28. Instagram also allows users to “follow” another user, which means that they receive updates about posts made by the other user. Users may also “unfollow” users, that is, stop following them or block them, which prevents the blocked user from following that user.
29. Instagram allow users to post and share various types of user content, including photos, videos, captions, comments, and other materials. Instagram collects and maintains user content that users post to Instagram or share through Instagram.
30. Instagram users may send photos and videos to select individuals or groups via Instagram Direct. Information sent via Instagram Direct does not appear in a user’s feed, search

history, or profile.

31. Users on Instagram may also search Instagram for other users or particular types of photos or other content.
32. For each user, Instagram also collects and retains information, called “log file” information, every time a user requests access to Instagram, whether through a web page or through an app. Among the log file information that Instagram’s servers automatically record is the particular web requests, any Internet Protocol (“IP”) address associated with the request, type of browser used, any referring/exit web pages and associated URLs, pages viewed, dates and times of access, and other information.
33. Instagram also collects and maintains “cookies,” which are small text files containing a string of numbers that are placed on a user’s computer or mobile device and that allows Instagram to collect information about how a user uses Instagram. For example, Instagram uses cookies to help users navigate between pages efficiently, to remember preferences, and to ensure advertisements are relevant to a user’s interests.
34. Instagram also collects and maintains information on the particular devices used to access Instagram. In particular, Instagram may record “device identifiers,” which includes data files and other information that may identify the particular electronic device that was used to access Instagram.
35. Instagram also collects other data associated with user content. For example, Instagram collects any “hashtags” associated with user content (i.e., keywords used), “geotags” that mark the location of a photo and which may include latitude and longitude information, comments on photos, and other information.
36. Instagram also may communicate with the user, by email or otherwise. Instagram collects and maintains copies of communications between Instagram and the user.
37. As explained herein, information stored in connection with an Instagram account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, an Instagram user’s account activity, IP log, stored electronic communications, and other data retained by Instagram, can indicate who has used or controlled the Instagram account. This “user attribution” evidence is analogous to the

search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the Instagram account at a relevant time. Further, Instagram account activity can show how and when the account was accessed or used. For example, as described herein, Instagram logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Instagram access, use, and events relating to the crime under investigation. Additionally, Instagram builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Instagram “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Instagram account owner. Last, Instagram account activity may provide relevant insight into the Instagram account owner’s state of mind as it relates to the offense under investigation. For example, information on the Instagram account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

38. Based on the information above, the computers of Instagram are likely to contain all the material described above with respect to the SUBJECT ACCOUNTS, including stored electronic communications and information concerning subscribers and their use of Instagram, such as account access information, which would include information such as the IP addresses and devices used to access the account, as well as other account information that might be used to identify the actual user or users of the account at particular times.

INVESTIGATION AND PROBABLE CAUSE

39. On May 22, 2024, the FBI received an online tip from Jane Doe One regarding her son, Minor Victim One (MV1), date of birth 08/02/2009. The tip indicated that MV1 had

been a victim in a sextortion scam. Jane Doe One noted that an unknown subject sent a text to MV1 containing an explicit and inappropriate photo of a girl and then requested a picture of MV1's "private parts" then began to threaten exposure if MV1 did not send money to the unknown subject. Jane Doe One further stated that extortionist used the phone number (972) 977-2851 and the email address Tobioyedokun9@gmail.com in their demands of MV1.

40. On May 24, 2024, an interview was conducted with Jane Doe One, during which, Jane Doe One stated the Instagram account that was used to extort MV1 was "ca_ssie800" with the name "Cassie".
41. Some of the chat messages between MV1 and the unknown **SUBJECT ACCOUNT** "Cassie" were obtained by law enforcement. In those messages, "Cassie" asked MV1 if MV1 wanted to "get freaky" to which MV1 asked the "Cassie" to start. "Cassie" then requested a photo of MV1 to get her "wet." MV1 and "Cassie" message back and forth about who will send the first photo, at which point, "Cassie" distributed to MV1 an image of a vagina. At that point, MV1 and "Cassie" appeared to get on a video call. After the call, "Cassie" sent MV1 one photograph of MV1 taking a selfie with face visible, one photograph of a penis, one photograph of an Instagram page, and one photograph of a telephone number.
42. "Cassie" then sent a message to MV1 which stated "I'm gonna send this pics to all your school pages Facebook and Instagram and all the pages in the city it both indicate live cam it gonna go viral so soon and to all your family and friends. You can stop talking and bluff then i will immediately, you just an option tho...I'm gonna send it to all your friends and family on insta right now. MV1 asked "if she was joking and "Cassie" responded "Do you think I'm joking...Pay me 200."
43. Hundreds of other messages were exchanged and, in summary, those messages revealed "Cassie" demanded money from MV1 and continued to threaten him that if he did not, she would make sure MV1's photograph of his penis went "viral."
44. On June 12, 2024, your affiant served a subpoena on Meta Platforms requesting subscriber records and IP tolls for the following: Instagram account username "ca_ssie800" and telephone number (972) 977-2851 as well as Google email account Tobioyedokun9@gmail.com. In response, Meta Platforms provided responsive records

that stated there were no records related to the telephone number. Meta did provide the following information about the “cassie800” Instagram account:

First Name:	Cassie
Vanity Name:	ca_ssie800
Registration Date:	2023-05-30 17:12:05 UTC
Registration Ip:	2600:1009:b03b:7949:a112:5a96:3c9d:cb06
Phone Numbers:	+2348072771368 Verified
Logins:	IP Address: 102.88.69.65 Time: 2024-05-24 22:29:44 UTC IP Address: 102.89.22.126 Time: 2024-05-19 21:00:43 UTC IP Address: 102.89.23.40 Time: 2024-05-19 20:59:48 UTC IP Address: 92.119.177.59 Time: 2024-05-18 23:43:58 UTC

Meta also provided the following information about the Tobioyedokun9@gmail.com too:

Account Type:	InstagramUser
Name: First:	Drew Cowther
Registered Email:	tobioyedokun9@gmail.com (Verified)
Vanity Name:	raven_cowther09
Registration Date:	2017-11-27 13:13:55 UTC
Registration IP:	96.39.217.161

45. Also on June 12, 2024, your affiant served a subpoena on AT&T requesting customer and subscriber records for telephone number (972) 977-2851, the number provided by Jane Doe One used to extort MV1. In response, AT&T provided the following information:

FINANCIAL LIABLE PARTY:

Name:	MARY JOLLEY
Credit Address:	514 JEFFERSON LN, LAKE DALLAS, TX 75065
Customer Since:	05/19/2024
Contact Home Email:	TOBIOYEDOKUN9@GMAIL.COM

USER INFORMATION:

MSISDN:	(972) 977-2851
IMSI:	310280121693406
MSISDN:	Active: 05/19/2024 - Current
Name:	MARY JOLLEY
User Address:	514 JEFFERSON LN, LAKE DALLAS, TX 75065
Service Start Date:	05/19/2024
Contact Home Email:	TOBIOYEDOKUN9@GMAIL.COM

46. Additionally, on June 12, 2024, your affiant served a subpoena on Google requesting subscriber records for email address tobioyedokun99@gmail.com, the email provided by Jane Doe One used to extort MV1. In response, Google provided the following information:

Google Account ID:	213883993223
Name:	Tobi Oye
Given Name:	Tobi
Family Name:	Oye
E-Mail:	tobioyedokun99@gmail.com
Created On:	2023-02-16 20:42:21 Z
Terms of Service IP:	197.211.59.126
Last Updated Date:	2024-04-17 05:23:10 Z
Recovery SMS:	+2349152274351 [NG]

47. On June 13, 2024, Jane Doe One emailed your affiant a screen-recording of the conversation MV1 had with the unknown target. Your affiant reviewed the recording which confirmed that MV1 was tricked into exposing his penis and then extorted with threats that he would need to pay the unknown target money, or the target would expose the penis of MV1 to family and friends. To facilitate payment, the extortionist provided MINOR VICTIM with the email addresses which included Oladimeji12340@gmail.com, plqkbxsqzdic@hotmail.com, ocbt642252@hotmail.com, and Tobioyedokun9@gmail.com.
48. On or about June 17, 2024, your affiant served a subpoena on PayPal requesting customer information for: plqkbxsqzdic@hotmail.com. In response, PayPal provided the following customer records which included four payment attempts from MV1 to the account holder on May 22, 2024, in amount of \$44.14 for each transaction.
49. Based on the information that has been gathered to date by your affiant, including interviews with the identified victim's mother noted above, law enforcement reports, subpoena requests and returns, and social media exchanges including, but not limited to, those taking place on Instagram, your affiant has reason to believe that the individual utilizing the **SUBJECT ACCOUNTS**, most likely an individual residing overseas, was threatening the noted victim in a bid to obtain nude or sexually explicit images and videos of them while also using child pornography images already obtained in a bid to gather more exploitation material. Therefore, it is likely that the **SUBJECT**

ACCOUNTS contains items which constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, 2252A – the sexual exploitation of a minor and possession of child pornography as well as 18 USC §875(d) – extortion via interstate communications.

**COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL
INTEREST IN CHILDREN**

50. Based on my own knowledge, experience, and training in online child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who have a sexual interest in minors and/or seek to sexually exploit minors via online communications:
- A. Those who have a sexual interest in minors, may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from discussions of or literature describing such activity.
 - B. Those who have a sexual interest in children and/or seek to sexually exploit minors via online communications may collect sexually explicit or suggestive materials in a variety of media. These materials are frequently used for the sexual arousal and gratification of the individual. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
 - C. Individuals who have a sexual interest in children have been found to: download, view, then delete child pornography on a cyclical and repetitive basis; view child pornography without downloading or saving it; or save child pornography materials to cloud storage.
 - D. Those who have a sexual interest in minors may correspond online with and/or meet others to share information about how to find child victims, exchange stories about their sexual exploits with children, and/or exchange child pornography materials; and tend to conceal and maintain in a safe, secure and

private environment such correspondence as they do any sexually explicit material related to their illicit sexual interest.

- E. When communications relating to a sexual interest in children, and/or child pornography files are stored on or accessed by computers and related digital media, forensic evidence of the accessing, downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such files have been deleted from the computers or digital media.

51. Based upon the conduct of individuals who have a sexual interest in children and/or seek to sexually exploit, coerce, or entice minors via online communications, as set forth in the above paragraphs, there is probable cause to believe that evidence of the violations of 18 U.S.C. §§ 2251, 2252, 2252A – the sexual exploitation of a minor and possession of child pornography as well as 18 USC §875(d) – extortion via interstate communications. is currently located on the **SUBJECT ACCOUNTS**.

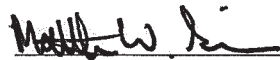
INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

52. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Instagram, LLC via Facebook, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment.

CONCLUSION


53. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252, 2252A – the sexual exploitation of a minor and possession of child pornography as well as 18 USC §875(d) – extortion via interstate communications, and evidence of those violations is located in the content of the **SUBJECT ACCOUNTS**. Your affiant respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT ACCOUNTS** described in Attachment A, and the seizure of the items described in Attachment B.

54. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Furthermore, because the warrant will be served on Instagram, LLC via Facebook, Inc., who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.



Matthew W. Guinn
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me 27th day of June, 2024.



Elizabeth A. Preston Deavers
United States Magistrate Judge

